UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; Does 1–15, *Defendants*.	Civil Action No. 1:21-cv-10260-DLC

DECLARATION OF LAURA HARRIS IN SUPPORT OF GOOGLE LLC'S REQUEST FOR ENTRY OF DEFAULT

I, Laura Harris, hereby declare and state as follows:

1. I am an attorney with the law firm of King & Spalding LLP ("King & Spalding") and counsel of record for Plaintiff Google LLC ("Google"). I am a member of good standing of the bar of New York. I make this declaration in support of Google's Request for Entry of Default. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. Defendants Are on Notice of This Action and Have Not Responded

2. As described more fully below, Defendants Dmitry Starovikov, Alexander Filippov, and John Doe Defendants 1–15 ("Defendants") have been properly served with the Complaint and Exhibit A thereto, the summons, the Motion for a Temporary Restraining Order ("TRO"), the Proposed TRO and Order to Show Cause Regarding a Preliminary Injunction, and all supporting evidence (collectively, the "TRO Documents") pursuant to the means authorized by the Court in the Temporary Restraining Order, ECF No. 8.

3. In light of (a) Google's efforts to serve Defendants by physical mail, email, and text message (including by WhatsApp), (b) widespread media coverage of this case, including in Russia, that specifically mentions Google's claims against Defendants Starovikov and Filippov, and (c) Google's disruption of the botnet's activity and Defendants actions in response thereto, Defendants have been on notice of this action since at least December 10, 2021. Yet, to date, Defendants have neither appeared in this case nor contacted Google or its counsel in connection with this lawsuit. Upon information and belief, the Defendants against whom entry of default

is sought are not infants or incompetent persons. I base this conclusion in part on the fact that Defendants have engaged in sophisticated acts of computer intrusion and theft of sensitive information from computer networks and have operated and procured sophisticated cybercrime infrastructure. I have seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

II. Service of Process

4. I oversaw Google's efforts to provide service and notice to the Defendants through the multiple channels identified below. As set forth in my declaration in support of the TRO Application, ECF No. 24, ¶ 8, prior to the TRO filing, Google's Threat Analysis Group ("TAG") conducted an investigation to identify the true identities of all persons responsible for operating the Glupteba botnet. This investigation revealed contact information associated with each Defendant—in particular, the physical mailing addresses, email addresses, and telephone numbers associated with Defendants and/or the entities, IP addresses, or domains under their control or otherwise associated with their criminal enterprise (the "Enterprise") or the Glupteba botnet. Defendants themselves provided certain of this information to Google and/or web hosting companies and domain registrars used by the Enterprise. Google used this information to attempt to serve Defendants by physical mail, email, and text messages.

a. Service by Mail

5. Google attempted to effectuate service by physical mail.

6. On December 8, 2021 at 6:00 pm ET, Google attempted to serve Defendants by FedEx at the following physical address that Google identified in its pre-filing investigation:

Dmitry Starovikov
123112, Moscow, Presnenskaya
Embankment 12, Office 5

Alexander Filippov
123112, Moscow, Presnenskaya
Embankment 12, Office 5

7. On December 21, 2021, FedEx issued a notification that it was unable to deliver the shipment to the address. As of February 7, 2022, FedEx labeled the shipments "undeliverable."

b. Service by Email

8. Google also attempted to effectuate service by email, as authorized by the TRO. The Court specifically provided that "good cause continues to exist to grant alternative service of the filings in this matter via . . . email . . . because Google establishes that traditional service methods would be futile." ECF No. 8, ¶ 18.

9. Google identified multiple email addresses associated with Defendants in its pre-filing investigation. Defendants have used these email addresses in registering the domains associated with the botnet.

10. I oversaw the process of sending notice of this lawsuit to each of the email addresses identified by Google in its pre-filing investigation. Each email attempting to effectuate service was sent by an attorney at King & Spalding with the following text:

> A lawsuit has been initiated against you in the United States District Court of the Southern District of New York. The following link contains copies of the restraining order, summons and complaint.
>
> https://drive.google.com/drive/folders/1bGIIKRQmgoVbh93t0JiGAKi-f2Dbiof3?usp=sharing
>
> Regards,
> King & Spalding LLP

11. King & Spalding attempted to effectuate service by email, as described above, on December 8, 2021, at approximately 9:00 pm ET.

12. On December 10, 2021, at approximately 4:00 pm ET, King & Spalding further attempted to notify Defendants by email that the "hearing on the motion for a preliminary injunction" had been "adjourned to 1 pm ET on December 16, 2021" and provided a link to a copy of the Court's order.

13. King & Spalding received delivery failure notifications for each of its emails. In one such instance, King & Spalding received a message that its email had been "blocked . . . due to [an] organization setting."

c. Service by Text Message

14. Google also attempted to effectuate service by text message as authorized by the TRO. The Court specifically provided that "good cause continues to exist to grant alternative service of the filings in this matter via . . . text . . . because Google establishes that traditional service methods would be futile." ECF No. 8, ¶ 18.

15. *Texts to Starovikov*: On December 9, 2021 at around 1:30 pm ET, and December 10, 2021 at 3:00 pm ET, I oversaw service of process by text message to a

phone number associated with Defendant Starovikov, as identified through Google's pre-filing investigation. King & Spalding received an "invalid number" error message in response to these efforts.

16. On December 9, 2021 and December 10, 2021, King & Spalding also attempted to effectuate service on Defendant Starovikov by text message through the WhatsApp messaging platform—specifically, through an account connected to one of the telephone numbers associated with Starovikov. King & Spalding did not receive a delivery failure notification or an error message in response to its WhatsApp message.

17. *Texts to Filippov*: On December 9, 2021 at around 1:30 pm ET, and December 10, 2021 at 3:00 pm ET, I oversaw service of process by text messages to two numbers associated with Alexander Filippov, as identified through Google's pre-filing investigation. King & Spalding did not receive any delivery failure notifications or error messages in response to the text messages sent to these numbers.

18. Each of the text messages and WhatsApp messages sent to Defendants contained the following message: "A lawsuit has been filed against you in the United States District Court for the Southern District of New York. This link contains a copy of a restraining order, summons, and complaint." The text messages sent on December 10, 2021 also informed the Defendants that the preliminary injunction hearing had been scheduled for December 16, 2021 and provided a link to a copy of the Court's order.

III. Additional Means of Notification

19. Upon information and belief, Defendants have actual notice of this proceeding given the impact of the TRO, the Preliminary Injunction Order, and Google's disruption efforts thereunder.

20. Following the Court's issuance of the TRO on December 7, 2021, Google began its efforts to suspend the Internet domains and IP addresses associated with Defendants' botnet and the Enterprise. As detailed in Google's January 31, 2022 Status Update, *see* ECF No. 32, Google's efforts have led to the suspension or disruption of nearly 100 domains and IP addresses associated with the Glupteba Enterprise, including but not limited to (i) all seven of the originally identified command-and-control servers ("C2 servers"), which the Enterprise uses to provide instructions to devices infected with the malware; (ii) fifteen domains associated with "storefronts" and developer recruitment sites that the Enterprise uses to effectuate illicit schemes; and (iii) fifty-seven domains associated with content delivery network servers ("CDN servers").

21. On or around December 13, 2021, Defendants ceased operating one of their most prominent storefronts, dont.farm, which the Enterprise had used to sell access to stolen Google user account information. Managers of dont.farm informed the storefront's customers that they were shutting down, and subsequently deleted the accounts that had been used to communicate with those customers. Further, in response to the suspension of Defendants' original C2 servers, Defendants have attempted to establish five new C2 servers and to direct infected devices to the

locations of these new C2 servers through the blockchain. Pursuant to the Court's orders, Google has taken action resulting in the suspension of all five new C2 servers.

22. Further, many of the world's most prominent newspapers and news websites have published stories concerning this case. Below are excerpts of this media coverage, including in Russia, detailing the claims against Defendants, including the alleged involvement of Defendants Starovikov and Filippov:

- "Google Filed A Lawsuit Against Two Russians Because Of Possible Participation In A Criminal Scheme," RUSSIAN NEWS AGENCY (Dec. 7, 2021), https://tass.ru/ekonomika/13137081 (Russian state media noting that Google "accused Dmitry Starovikov and Alexander Filippov, along with 15 other unnamed individuals, of creating the Glupteba botnet").

- J. Tarabay, "Google Sues Two Russians For Alleged Organised Crime Enterprise," ALJAZEERA (Dec. 7, 2021), https://www.aljazeera.com/economy/2021/12/7/google-sues-two-russians-for-alleged-organised-crime-enterprise ("In a complaint being unsealed Tuesday in the United States District Court for the Southern District of New York, Google names two defendants, Dmitry Starovikov and Alexander Filippov, as well as 15 unnamed individuals.").

- G. Vynck, "Google Disrupted A Massive Botnet That Hackers Used To Steal Information And Mine Cryptocurrency," THE WASHINGTON POST (Dec. 7, 2021), https://www.washingtonpost.com/technology/2021/12/07/google-glupteba-botnet-hack/ ("Google's lawsuit names two people — Dmitry Starovikov and Alexander Filippov — who it alleges are among the leaders who control the Glupteba network.").

- "Google Sues Alleged Russian Cyber Criminals," BBC NEWS (Dec. 7, 2021), https://www.bbc.com/news/world-us-canada-59571417 ("According to a lawsuit filed in New York and unsealed on Tuesday, the botnet built by Dmitry Starovikov, Alexander Filippov and their associates has become a 'modern technological and borderless incarnation of organised crime.'")

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge

Executed on February 7, 2022 in New York, New York.

/s/ Laura Harris
Laura Harris